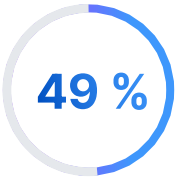
Pourquoi choisir Jamf for Mac

Les responsables informatiques des entreprises ont une lourde mission : limiter les temps d'arrêt des appareils et préserver la productivité et la satisfaction des utilisateurs finaux, tout en réduisant l'exposition aux risques et en repoussant les cybermenaces.

À l'heure où de plus en plus d'employés choisissent le Mac, les équipes informatiques sont tenues d'offrir des expériences simples et une sécurité de haut niveau, sans faire de compromis ni dépasser les budgets impartis. C'est là que Jamf entre en jeu.

Les équipes informatiques consacrent trop de temps aux tâches informatiques de routine.

L'environnement informatique moderne exige de la rapidité, mais les workflows obsolètes, les outils déconnectés et le manque de données en temps réel font perdre énormément de temps aux équipes. Cette approche n'est pas viable à grande échelle.

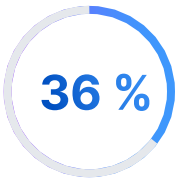


des organisations se plaignent de difficultés à accéder aux informations en temps voulu [1]

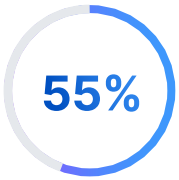
Sans visibilité sur les appareils, les équipes informatiques perdent du temps à réunir les données de simples rapports en utilisant des solutions approximatives et des appels d'API manuels. L'absence de données en temps réel fait également peser un risque accru sur la sécurité des appareils.

des responsables informatiques voient dans les défis d'intégration un frein aux initiatives de transformation numérique [2]

En l'absence d'une documentation claire, d'intégrations natives ou d'un cadre de développement clair, les équipes informatiques perdent beaucoup de temps à coordonner leurs outils.



des Mac n'avaient pas activé FileVault [3]



des Mac n'avaient pas activé FileVault [3]

Les équipes informatiques perdent beaucoup de temps à renforcer manuellement les appareils et à corriger les problèmes qui nuisent à la conformité. Les modèles de conformité proposés par les autres fournisseurs sont souvent incomplets, ou ils ne respectent pas le projet de conformité de macOS en matière de sécurité (mSCP). Toutes ces lacunes alourdissent la charge des équipes informatiques.

Le niveau de risque des environnements Apple augmente chaque année.

La popularité accrue de Mac en entreprise a un revers : malgré la difficulté, les pirates informatiques estiment désormais que le piratage des appareils Apple en vaut la peine.

Sans une protection contre les menaces spécifiques à Apple, l'exposition aux risques ne fait que s'accentuer. Lorsque les données de télémétrie n'incluent pas les événements propres à Mac (ceux de Gatekeeper et XProtect en particulier), vous n'avez qu'une visibilité limitée sur les menaces, et devez attendre que les pirates alertent d'autres contrôles de sécurité. Dépourvus d'équipes de recherche des menaces dédiées à Apple, la plupart des fournisseurs de sécurité ne sont pas à la hauteur de l'enjeu.

Le coût moyen d'une infraction aux réglementations en matière de protection des données est de 14,8 millions de dollars.[2]

L'absence de journaux et de pistes d'audit détaillés empêche l'entreprise de se préparer correctement aux audits. À l'opposé, les intégrations avec les fournisseurs de SIEM apportent une visibilité supplémentaire qui permet de profiter d'une interface de sécurité unique et complète.

39 % des organisations comptent dans leur parc au moins un appareil présentant des vulnérabilités connues ;[3] une visibilité limitée sur les CVE et l'absence de workflows d'application automatique des correctifs vous exposent aux vulnérabilités logicielles.

300

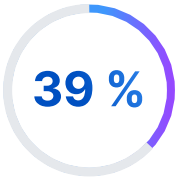
Jamf Threat Labs suit plus de 300 familles de logiciels malveillants sur macOS [3]

21

Jamf Threat Labs a identifié 21 nouvelles familles de logiciels malveillants pour la seule année 2023 [3]

14,8 M$

Le coût moyen d'une infraction aux réglementations en matière de protection des données



des organisations comptent dans leur parc au moins un appareil présentant des vulnérabilités connues [3]

Pourquoi Jamf for Mac ?

Jamf augmente deux fois plus la productivité des équipes que ses concurrents [4] en s'intégrant en toute simplicité à n'importe quelle infrastructure informatique. Cette approche allège en effet les étapes de collecte des données et réduit la fréquence des pannes, les besoins d'assistance de niveau 1 et les opérations manuelles.

Parce qu'elles ciblent les menaces spécifiques à Apple, accélèrent la réponse, atténuent les vulnérabilités non corrigées et renforcent la conformité, nos solutions de sécurité réduisent l'exposition aux risques deux à trois fois plus que leurs concurrents.

Nous y parvenons en agissant sur plusieurs leviers :

- Surveillance des menaces en temps réel sur de multiples vecteurs avec l'appui d'équipes de recherche des menaces dédiées à Apple
- Riches capacités d'inventaire, de création de rapports, de journalisation et de suivi d'audit.
- Nombreuses intégrations préétablies avec des outils de gestion et de sécurité informatiques
- Un cadre de règles robuste avec exécution automatique en temps réel et Self Service pour l'utilisateur final
- Acquisition, validation, reconditionnement et déploiement automatisés des applications

Nos équipes d'assistance et de service sont réputées pour la qualité de leurs prestations. Mais Jamf, c'est aussi Jamf Nation, le plus grand forum d'administrateurs Apple au monde, où les membres échangent et partagent leur vaste expertise.

« L'excellente assistance technique que m'apporte Julie [ingénieure de support technique] me rappelle à quel point nous avons bien fait de choisir Jamf pour la gestion des Mac. Je n'ai aucun problème à démontrer à ma direction que Jamf est un partenaire de confiance.

– Analyste informatique au sein d'une administration

Jamf accroît davantage la productivité que d'autres solutions.

Jamf devance ses concurrents à plusieurs titres :

- Réduction des temps d'arrêt des appareils
- Augmentation de l'efficacité des opérations informatiques
- Diminution des besoins d'assistance utilisateur directe
- Meilleur suivi et visibilité plus détaillée

Mise en production plus rapide

L'accès en temps réel à des informations complètes sur les appareils l'automatisation des workflows allègent les tâches de reporting manuel, d'audit et de gestion des workflows.

Comment ?

- **Les workflows d'intégration automatisés** définissent des configurations en fonction du rôle, du service, de l'utilisateur et de la localisation ; le service informatique gagne du temps et les nouveaux employés sont immédiatement opérationnels.
- **Le ciblage précis** facilite l'automatisation du dépannage, le renforcement des appareils et les mises à jour logicielles : un gain de temps pour l'utilisateur final comme pour le service informatique.
- **L'assistance de niveau 1** ne s'arrête pas aux fonctions de base et permet aux utilisateurs d'ajouter des applications en libre-service pour devenir plus productifs.

Jamf réduit davantage les risques que les autres.

L'infrastructure de règles de Jamf englobe des cadres de gestion des appareils, l'exécution de scripts basée sur des règles et des contrôles du réseau. Notre équipe d'experts en recherche des menaces s'appuie sur des analyses comportementales entraînées avec soin pour neutraliser les attaques qui ciblent spécifiquement Apple.

Avec Jamf, les responsables informatiques peuvent :

- Bloquer les menaces « zero day » connues et émergentes qui ciblent spécifiquement Apple
- Réagir plus rapidement aux risques de sécurité en exécutant en temps réel des mesures de remédiation ciblées
- Limiter les vulnérabilités non corrigées grâce aux rapports CVE et à la mise à jour automatique des logiciels et des applications
- Réduire la probabilité de perte de données grâce à une connectivité sécurisée conçue pour Apple, qui évalue les risques de façon dynamiques en s'appuyant sur une quantité croissante d'informations
- Automatiser le durcissement des appareils par l'intégration du projet de conformité de macOS en matière de sécurité, l'élimination de l'erreur humaine et une meilleure préparation aux audits grâce à des journaux et des pistes détaillés.

---

1. *« Automation: Trends, Challenges and Best Practices », IDC, 2023*
2. *« State of IT Report », troisième édition, Salesforce*
3. *« Jamf Security 360 : Rapport annuel sur les tendances 2024 », Jamf, 2024*
4. *« Driving ROI: The Case for a Proven Apple Enterprise Management Solution », livre blanc Jamf, 2021.*

Jamf est votre meilleure option. Mais ne nous croyez pas sur parole.

Avis G2 :

« Jamf Pro reste la référence de la gestion des appareils mobiles pour Apple et Mac. »

« Un soutien unanime de la part des fournisseurs. Jamf est couramment cité dans la documentation fournisseur, car c'est le produit de référence pour la MDM Apple. »

jamf

Essayez Jamf